MATHEMATICS

THE FREE PRODUCT OF A QUADRATIC NUMBER FIELD AND A SEMI-FIELD.

BY

T. H. M. SMITS

(Communicated by Prof. J. G. VAN DER CORPUT at the meeting of December 21, 1968)

§ 1. INTRODUCTION

The general structure of free products of rings and fields [1]) has been described extensively by P. M. COHN, cf. [5, 7, 8]. E.g. the free product of any family of rings over an amalgamated subfield C exists [4, Theorem 4.7] and when the rings have no zero-divisors, then their free product also has no zero-divisors [5, Theorem 2.5]. Further we mention the important result: Let P be the free product of a family of fields over an amalgamated subfield C, then:

(i) every unit of P is a monomial unit, i.e. a product of elements from the fields [5, Theorem 2.6];

(ii) P is a *UFD* (unique factorization domain) [7, Corollary 2, p. 356].

(iii) P is a "fir" (free ideal ring) [8, Theorem 4.3].

In [6] COHN studied the structure of the free product of two (noncommutative) quadratic extensions of a given field C. This free product appeared to be a left *PID* (principal ideal domain) [6, Lemma 2, left dimension two].

In this paper we describe the structure of the free product P of the quadratic field $K_1=C(\sqrt{\gamma_1})$ and the (commutative) ring $R_2=C[\xi]/(\xi^2-\gamma_2)$ with $\gamma_1, \gamma_2 \in C$. If γ_2 is not the square of an element of the field C then R_2 is a field and we have the situation described by Cohn, otherwise R_2 is a ring with zero-divisors. When $\gamma_2 \neq 0$ the ring R_2 is a direct sum of two copies of C. Such a ring has been called a "semi-field" by Albert [2, p. 81]. Now in particular we have the following results.

I. If γ_2 is not a perfect square, then P is a *PID* (left and right) and the quotient field $Q(P)$ of P is a division algebra of order 4.

II. If γ_2 is a square, say $\varrho^2 (\varrho \in C)$, then P is a Noetherian prime ring and the quotient ring $Q(P)$ of P is a cyclic algebra and a total matrix algebra. It is also the tensor (direct) product of two four dimensional central division algebras, provided that C is the field of rational numbers.

[1]) The term "field" will be used in the sense of "skew field", i.e. "not necessarily commutative division ring".

§ 2. Polynomials

The theory of non-commutative (skew) polynomials has turned out to be very useful in the theory of cyclic algebras, crossed products etc. That's why we first introduce some abbreviations and notations concerning skew polynomials. Given a field L, an endomorphism σ and a nilpotent σ-derivation Δ, satisfying $\Delta^2=0$ and

$$(ab)\Delta = a\Delta\cdot b\sigma + a\cdot b\Delta \qquad (a, b \in L);$$

we denote by $L[x; \Delta\sigma, \sigma, 0]$ the ring of skew polynomials in an indeterminate x subject to the commutation formula

$$x\cdot a = (a\Delta\sigma)x^2 + (a\sigma)x \qquad (\text{all } a \in L).$$

In the same way, given a field L, an endomorphism σ and a $(1, \sigma)$-derivation $\bar{\delta}$ of L, satisfying

$$(ab)\bar{\delta} = a\bar{\delta}\cdot b + a\sigma\cdot b\bar{\delta} \qquad (a, b \in L),$$

then we denote by $L[x; 0, \sigma, \bar{\delta}] = L[x; \sigma, \bar{\delta}]$ the ring of skew polynomials in an indeterminate x subject to the commutation formula

$$x\cdot a = (a\sigma)x + a\bar{\delta} \qquad (\text{all } a \in L).$$

Both rings turn out to be a left principal ideal domain with a right Euclidean algorithm and also a unique factorization domain. If σ is an automorphism of L, then they are non-commutative principal ideal domains (left and right), cf. [24, Theorem 4] and [14, Chapter 3].

The skew polynomial ring with the general product rule

$$x\cdot a = (a\delta_2)x^2 + (a\delta_1)x + (a\delta_0) \qquad (\text{all } a \in L)$$

is denoted by $L[x; \delta_2, \delta_1, \delta_0]$, where $\delta_0, \delta_1, \delta_2$ are certain mappings in the coefficient field L. In general this ring has zero-divisors, idempotent and nilpotent elements, and is not a left *PID*. For even a more general situation we prove the following important theorem.

Theorem 1. *Let R be the ring of skew polynomials in an indeterminate x, $\sum a_i x^i$ over a field L, with the usual addition and a multiplication defined by*

$$\begin{cases} x\cdot a = (a\delta_0) + (a\delta_1)x + \dots + (a\delta_{r-1})x^{r-1} + (a\delta_r)x^r, \\ x^r\cdot a = (aT)x^r \qquad (\text{all } a \in L,\ r \text{ is a fixed integer}), \end{cases}$$

where $\delta_0, \delta_1, \dots, \delta_r$ are certain mappings in the field L and T is an endomorphism of L. For the ring R the following statements hold:

(i) *the left quotient ring $Q(R)$ of R is a left Artinian simple ring;*
(ii) *R is a left Noetherian prime ring.*

Proof. Every polynomial $f \in R$ may be written into the form

$$f = b_0 + b_1 x + b_2 x^2 + \dots + b_{r-1}x^{r-1}, \qquad b_i \in A = L[x^r; T, 0],$$

where the ring A is a left Noetherian principal ideal domain, cf. JACOBSON [14], Chapter 3. So we may write

$$R = A + Ax + Ax^2 + \dots + Ax^{r-1}.$$

Because R is finitely generated over the left Noetherian ring A we observe that the ring R is left Noetherian. In fact it is easy to see that every left ideal of R is generated by at most r elements.

To construct the left quotient ring $Q(R)$ of R we first embed the ring A in a left quotient field $A^* = L(x^r; T, 0)$ and then transform the left A^*-vector space

$$R^* = A^* + A^*x + A^*x^2 + \dots + A^*x^{r-1}$$

into a ring by extending the multiplication in R to R^* (this is possible only in one way). Now R^* has become the left quotient ring of R, because if $d \in R^*$ is not a right zero-divisor, then d has a left inverse d^1 in R^* (cf. JACOBSON [15], p. 158, Prop. 2). However R^* is a left Artinian ring with a unity element, so whenever $d^1 d = 1$, we also have $dd^1 = 1$ (DIVINSKY [9], p. 32), i.e. R^* is the left quotient ring $Q(R)$ of R. Finally a well-known theorem of Goldie states that if $Q(R)$ is a left Artinian simple ring, then the ring R is a prime ring, cf. HERSTEIN [12], Theorem 7.2.3., p. 177. This proved (ii).

§ 3. THE FREE PRODUCT

Let K_1 be a (commutative) quadratic extension of a field C, generated by a_1 over C, and defining equation

$$(1) \qquad a_1^2 = \gamma_1 \qquad (\gamma_1 \in C),$$

i.e. K_1 is the quadratic field $C(\sqrt{\gamma_1})$.

Let us define the automorphism S_1 of K_1 by putting

$$(2) \qquad (\alpha + \beta a_1)S_1 = \alpha - \beta a_1 \qquad (\alpha, \beta \in C).$$

Further we introduce the S_1-derivation D_1 by putting

$$(3) \qquad (\alpha + \beta a_1)D_1 = \beta \qquad (\alpha, \beta \in C).$$

We observe that $D_1^2 = 0$, $D_1 S_1 + S_1 D_1 = 0$, cf. [23]. Next we introduce the second ring R_2, generated by a_2 over C and defining relation

$$(4) \qquad a_2^2 = \gamma_2 \qquad (\gamma_2 \in C).$$

Now we consider the structure of the free product

$$P = K_1 \star R_2$$

of the field K_1 and the ring R_2 over the common subfield C. The structure of the ring P turns out to depend strongly on the structure of the ring R_2. However we first have the following general theorem (cf. COHN [6], p. 548 for the case of two quadratic extension fields).

Theorem 2. $P = K_1[x; D_1S_1, S_1, (\gamma_1 - \gamma_2)D_1S_1]$ and the center of P is the (commutative) polynomial ring $C[x^2]$.

Proof. First we derive the commutation formulas. Put

$$x = a_1 - a_2, \tag{5}$$

so $\gamma_1 - xa_1 - a_1x + x^2 = (a_1 - x)^2 = a_2{}^2 =$

$$= \gamma_2, \text{ hence}$$

$$x \cdot a_1 = x^2 - a_1x + (\gamma_1 - \gamma_2),$$

and from $x^2 \cdot a_1 = x(xa_1)$ we easily have

$$x^2 \cdot a_1 = a_1x^2.$$

The remaining part of the proof we can easily copy from COHN [6], p. 549. For it follows that these left-hand polynomials in x (over K_1) form a subring P^1 of P. Clearly P^1 contains K_1 and because of

$$\alpha a_2 + \beta = -\alpha x + (\alpha a_1 + \beta) \qquad (\alpha, \beta \in C),$$

P^1 also contains the ring R_2; therefore P^1 coincides with P, because P is generated by K_1 and R_2. Thus every element of P may be written as a left-hand polynomial in x with coefficients from the field K_1. To prove the uniqueness, suppose that

$$c_0 + c_1x + c_2x^2 + \ldots + c_nx^n = 0 \qquad (c_j \in K_1, \; c_n \neq 0).$$

On multiplying by c_n^{-1} on the left we obtain a relation

$$b_0 + b_1x + b_2x^2 + \ldots + b_{n-1}x^{n-1} + x^n = 0 \qquad (b_j \in K_1).$$

However $x^n = (a_1 - a_2)^n$ contains a term of the form

$$a_2a_1a_2a_1 \ldots a_2a_1(a_2) \qquad (n \text{ factors})$$

which does not occur in any other term b_jx^j, contradiction, so every element of the free product P can be written uniquely as a polynomial in x and the theorem follows. We rewrite again the multiplication formulas:

$$x \cdot a_1 = x^2 - a_1x + (\gamma_1 - \gamma_2), \tag{6}$$

$$\left\{ \begin{array}{ll} x(\alpha + \beta a_1) = \beta x^2 + (\alpha - \beta a_1)x + \beta(\gamma_1 - \gamma_2) & (\alpha, \beta \in C), \\ x \cdot a = (aD_1S_1)x^2 + (aS_1)x + (\gamma_1 - \gamma_2)(aD_1S_1) & (a \in K_1), \end{array} \right. \tag{7}$$

$$x^2 \cdot a = ax^2 \qquad (\text{all } a \in K_1). \tag{8}$$

Also we have the following representation of P.

Theorem 3. $P = A[u; \sigma, \delta]/(u^2 - \gamma_2)$; $\sigma^2 = 1$, $\delta^2 = 0$; where $A = K_1[x^2]$ and $(u^2 - \gamma_2)$ is the 2-sided ideal generated by the polynomial $u^2 - \gamma_2$, which lies in the center of the ring $A[u; \sigma, \delta]$.

Proof. From the relation

$$x^2 \cdot a = ax^2 \qquad (\text{all } a \in K_1)$$

it follows immediately that the ring $A = K_1[x^2]$, generated by x^2 over the field K_1, is a commutative polynomial ring lying in the polynomial ring P (the free product, Theorem 2). Of course every polynomial f in P may be written uniquely into the form

$$\begin{aligned} f &= \alpha + \beta x & (\alpha, \beta \in A = K_1[x^2]) \\ &= (\alpha + \beta a_1) + \beta(x - a_1) = \\ &= (\alpha + \beta a_1) - \beta a_2 = \\ &= \bar{\alpha} + \bar{\beta} a_2 & (\bar{\alpha}, \bar{\beta} \in A). \end{aligned}$$

Now we derive the product formulas. We have

$$\begin{aligned} a_2 \cdot a_1 &= (a_1 - x)a_1 = a_1{}^2 - (xa_1) = \\ &= \gamma_1 - (x^2 - a_1 x + \gamma_1 - \gamma_2) = \\ &= -x^2 + a_1 x + \gamma_2 = \\ &= -x^2 + a_1(a_1 - a_2) + \gamma_2 = \\ &= -a_1 a_2 + (\gamma_1 + \gamma_2 - x^2), \end{aligned}$$

so

$$a_2 \cdot a_1 = -a_1 a_2 + (\gamma_1 + \gamma_2 - x^2). \tag{9}$$

We observe that an arbitrary element of the ring $A = K_1[x^2]$ may be written into the form $\theta_1 a_1 + \theta_2$, where $\theta_1, \theta_2 \in C[x^2]$. From the previous multiplication formula (9) we now easily derive

$$a_2(\theta_1 a_1 + \theta_2) = (-\theta_1 a_1 + \theta_2) a_2 + \theta_1(\gamma_1 + \gamma_2 - x^2). \tag{10}$$

Next we introduce the automorphism σ of the ring $A = K_1[x^2]$ by

$$(\theta_1 a_1 + \theta_2)\sigma = -\theta_1 a_1 + \theta_2 \qquad (\theta_1, \theta_2 \in C[x^2]) \tag{11}$$

and also the $(1, \sigma)$-derivation δ by

$$(\theta_1 a_1 + \theta_2)\delta = \theta_1(\gamma_1 + \gamma_2 - x^2). \tag{12}$$

Obviously $\sigma^2 = 1$, $\delta^2 = 0$ and the multiplication formula (10) may be written as

$$a_2 \cdot c = (c\sigma) a_2 + (c\delta) \qquad (\text{all } c \in A = K_1[x^2]). \tag{13}$$

In short, every element $f \in P$ may be written uniquely into the form

$$f = c_1 + c_2 a_2 \qquad (c_1, c_2 \in A), \tag{14}$$

where

$$a_2{}^2 = \gamma_2 \qquad (\gamma_2 \in C), \tag{15}$$

and the multiplication is defined by (13). This proves the theorem.

The following theorem indicates a relationship between the free product

P and the theory of cyclic algebras. However to get a better understanding of this theorem we first consider two lemmas. In the following let B be the skew polynomial ring over the field K_1 in an indeterminate y (which will be defined later) and with a multiplication defined by the relation

$$y(\alpha+\beta a_1)=\beta y^2+(\alpha-\beta a_1)y \qquad (\alpha, \beta \in C), \tag{16}$$

in particular

$$y a_1 = y^2 - a_1 y, \tag{17}$$

$$y\alpha=\alpha y \qquad (\alpha \in C), \tag{18}$$

$$y^2 b = b y^2 \qquad (\text{all } b \in B). \tag{19}$$

Of course we could have said immediately

$$B=K_1[y; D_1S_1, S_1, 0]. \tag{20}$$

From section 2 we know that the ring B is a PID (left and right), which has a quotient field

$$\begin{aligned} E=Q(B)&=K_1(y; D_1S_1, S_1, 0)\\ &=K_1(y^{-1}; S_1, D_1), \text{ cf. [24], p. 210.}\end{aligned}$$

The automorphism S of the ring B defined by

$$a_1S=y-a_1,\ yS=y \tag{21}$$

may be extended to the quotient field E.

Now we are ready to prove the following two lemmas.

Lemma 1. The quotient field E of B is a non-commutative cyclic field and a cyclic division algebra of order 4.

Proof. From the product formula $y\cdot a_1=y^2-a_1y$ and $a_1{}^2=\gamma_1$ we conclude that the field E is "governed" by the two relations

$$(y-a_1)^2=\gamma_1$$

and

$$a_1{}^2=\gamma_1.$$

The automorphisms of the field E (which leave fixed the elements of the subfield C) form a group, which consists of four elements:

$\mathrm{Aut}_C(E)=(I, T_1, T_2, T_3),\ T_3=T_1T_2=T_2T_1,$

and

$$T_1{}^2=T_2{}^2=T_3{}^2=I, \text{ the identity automorphism.}$$

The automorphisms T_i are defined by

$$S=T_1\colon\begin{cases}a_1\to y-a_1\\ y\to y\end{cases},\quad T_2\colon\begin{cases}a_1\to -a_1\\ y\to -y\end{cases},\quad T_3\colon\begin{cases}a_1\to a_1-y\\ y\to -y\end{cases}.$$

Hence

$$\mathrm{Aut}_{C(y)}(E)=(I,S),\ S^2=I,$$

where the field of rational "functions" of y is the set of elements left fixed by S. By AMITSUR [3], p. 87, we conclude that $E=Q(B)$ is a cyclic extension of order 2 of the subfield $C(y)$. In fact we have

$$E=C(y)+C(y)a_1=C(y)+a_1C(y). \tag{22}$$

The quotient field E of B is also a cyclic division algebra of order 4 over its center $C(y^2)$. We have

$$E=C(y^2)+C(y^2)a_1+C(y^2)y+C(y^2)a_1y, \tag{23}$$

so the elements $\{1, a_1, y, a_1y\}$ constitute a basis over the center $C(y^2)$. This concludes the proof of the lemma. The following lemma gives a connection with old theories.

Lemma 2. Let C have characteristic not two, then E is a quaternion algebra over $C(y^2)$.

Proof. Let $w=a_1-\frac{1}{2}y$, then it follows immediately from (17) that

$$w^2=\gamma_1-\tfrac{1}{4}y^2\in C(y^2),$$
$$yw=-wy.$$

Now it is easy to see that the $C(y^2)$-basis $(1, y, a_1, ya_1)$ may be replaced by $(1, y, w, yw)$.

Hence

$$Q(B)=E=C(y^2)+C(y^2)y+C(y^2)w+C(y^2)yw,$$

$$y^2\in C(y^2),\ w^2=\gamma_1-\tfrac{1}{4}y^2\in C(y^2),\ yw=-wy. \tag{24}$$

This kind of algebra has been called a (generalized) quaternion algebra, cf. ALBERT [2], p. 146.

Involuntary we remember some theorems which Claiborne Latimer and Miss Grace Shover derived in $\pm$ 1933 for these algebras. (The author guesses it is Mrs. Shover nowadays). Although we know already that the ring B is a *PID* we mention (cf. LATIMER [18], Theorem 1, p. 322): "Let $\bar{E}$ be a rational generalized quaternion algebra with a negative fundamental number and let $\bar{B}$ be an arbitrarily chosen set of integral elements in $\bar{E}$. Every one-sided ideal in $\bar{B}$ is principal".

Further let M be a rational semi-simple algebra of order n and G is a domain of integrity of order n in M. We now have (cf. G. SHOVER [22], Theorem 2, p. 614): "The number of classes of left ideals in G (the left class number) is equal to the right class number". LATIMER also proved (cf. [16], Theorem 1, p. 434):

"The number of classes of right ideals in G is finite". So by the result of Miss Shover also the left class number is finite and is equal to the right class number. It is tempting to generalize these theorems for our more general quaternion algebra, however we shall not do this here and we continue with a remarkable property of the free product P.

Theorem 4. If $\gamma_2 \neq 0$, then $P = B[v; S, 0]/(v^2-\gamma_2)$, where $(v^2-\gamma_2)$ is the 2-sided ideal generated by the polynomial $v^2-\gamma_2$, which lies in the center of the ring $B[v; S, 0]$.

Proof. Let
$$\begin{aligned} y &= a_1 + a_2a_1a_2^{-1} = a_1 + \gamma_2^{-1}a_2a_1a_2 = \\ &= \gamma_2^{-1}(a_2^2a_1 + a_2a_1a_2) = \\ &= \gamma_2^{-1}a_2(a_2a_1 + a_1a_2) = \\ &= \gamma_2^{-1}(x-a_1)\{(x-a_1)a_1 + a_1(x-a_1)\} = \\ &= \gamma_2^{-1}(x-a_1)\{x^2 - a_1x + \gamma_1 - \gamma_2 - \gamma_1 + a_1x - \gamma_1\} = \\ &= \gamma_2^{-1}(x-a_1)(x^2-\gamma_1-\gamma_2). \end{aligned}$$

Hence

$$(25)\quad \left\{ \begin{aligned} y &= \gamma_2^{-1}(x-a_1)(x^2-\gamma_1-\gamma_2) = \\ &= \gamma_2^{-1}(x^2-\gamma_1-\gamma_2)(x-a_1) = \\ &= -\gamma_2^{-1}a_2(x^2-\gamma_1-\gamma_2) = \\ &= \gamma_2^{-1}x^3 - \gamma_2^{-1}a_1x^2 - (\gamma_2^{-1}\gamma_1+1)x + (\gamma_2^{-1}\gamma_1+1)a_1. \end{aligned} \right.$$

By easy calculations it follows that for $n = 0, 1, 2, \ldots$

$$y^{2n} = \gamma_2^{-n}(x^2-\gamma_1-\gamma_2)^{2n} \text{ has degree } 4n \text{ in } x$$

and

$$y^{2n+1} = \gamma_2^{-n-1}(x^2-\gamma_1-\gamma_2)^{2n+1}(x-a_1) \text{ has degree } (4n+3) \text{ in } x.$$

However

$$a_2y^{2n} = y^{2n}a_2 = y^{2n}(a_1-x) \text{ has degree } (4n+1) \text{ in } x$$

and

$$a_2y^{2n+1} = y^{2n+1}a_2 = -\gamma_2^{-n}(x^2-\gamma_1-\gamma_2)^{2n+1} \text{ is a polynomial of degree } (4n+2) \text{ in } x.$$

So every polynomial $f \in P$ may be written uniquely into the form $\alpha + \beta a_2 (a_2^2 = \gamma_2)$, where α and β are polynomials in y and left-hand coefficients from K_1. Next we determine the commutation formulas. We successively have

$$y = a_1 + a_2a_1a_2^{-1},$$

hence

$$(y-a_1)^2 = (a_2a_1a_2^{-1})^2 = \gamma_1,$$

so

$$y^2 - ya_1 - a_1y + a_1^2 = \gamma_1,$$

thus

$$(26)\qquad ya_1 = y^2 - a_1y.$$

Only this last relation gives us the right to identify the polynomial ring in y with the ring B we considered in the previous two lemmas! Further we derive

$$a_2 \cdot a_1 = (a_2a_1a_2^{-1})a_2 = (y-a_1)a_2,$$

hence

$$a_2 \cdot a_1 = (y - a_1)a_2 = (a_1 S)a_2 \tag{27}$$

and also

$$a_2 \cdot y = y a_2 = (yS)a_2, \tag{28}$$

where we used the relations (21).

Altogether, every element $f \in P$ may be written uniquely into the form

$$f = b_1 + b_2 a_2 \qquad (b_1, b_2 \in B)$$

and the product is defined by

$$a_2 \cdot b = (bS)a_2 \qquad (\text{all } b \in B),$$

where we remember that $a_2^2 = \gamma_2 \in C$.

To say it in a more transparent way. The free product P may be considered as a left (or right) B-module, whose basis consists of the two elements $\{1, a_2\}$, so

$$P = B + Ba_2 = B + a_2 B; \qquad a_2^2 = \gamma_2 \in C; \tag{29}$$

in which the ring B is a principal ideal domain and products are defined by

$$a_2 \cdot b = (bS)a_2 \qquad (\text{all } b \in B)\ ^{1)}. \tag{30}$$

This remark completes the proof of Theorem 4 and leads us immediately to the following statement.

Theorem 5. The quotient ring (or quotient field) $Q(P)$ of P is a cyclic algebra (E, S, γ_2) over the field E and an algebra of order 4 over its center.

Proof. From $P = B + Ba_2$ we immediately conclude that

$$Q(P) = E + Ea_2, \tag{31}$$

where E is again the quotient field of the ring B. Because of Lemma 1 and the relations

$$\begin{cases} a_2 \cdot b = (bS)a_2 & (\text{all } b \in E), \\ a_2^2 = \gamma_2 \in C, \ S^2 = 1, \end{cases} \tag{32}$$

we observe that $Q(P)$ is a cyclic algebra over the field E, cf. HASSE [11], p. 172, JACOBSON [13] or ALBERT [2], p. 75, who gives the notation

$$Q(P) = (E, S, \gamma_2). \tag{33}$$

The center of P (regarded as a polynomial ring in x over K_1) is the ring $C[x^2]$. More precisely

$$P = C[x^2] + C[x^2]x + C[x^2]a_1 + C[x^2]a_1 x, \tag{34}$$

1) If $\gamma_2 = 0$, then ROBSON [19] calls such a ring P a "Hilbert polynomial ring over B of index 2", cf. [19], p. 134.

hence

$$Q(P) = C(x^2) + C(x^2)x + C(x^2)a_1 + C(x^2)a_1x, \tag{35}$$

where $C(x^2)$ is the quotient field of $C[x^2]$. From this relation we derive that the quotient ring (or field) is an algebra of order 4 over its center, which completes the proof of Theorem 5.

§ 4. Examples and special cases

Finally we have to say something about the element γ_2 of the common subfield C. Let $\sqrt{\gamma_2}$ denote an element of the field K_1 with the property

$$(\sqrt{\gamma_2})^2 = \gamma_2.$$

Of course in general such an element does not exist in the field K_1. In fact we have the following four cases.

1. $\sqrt{\gamma_2} = \alpha_1 + \beta_1 a_1 = s_1 \in K_1, \notin C$ $(\alpha_1, \beta_1 \in C, \beta_1 \neq 0)$. From

$$s_1^2 = (\alpha_1 + \beta_1 a_1)^2 = \alpha_1^2 + \beta_1^2\gamma_1 + 2\alpha_1\beta_1 a_1 = \gamma_2$$

we immediately observe that $2\alpha_1\beta_1 = 0$ $(\beta_1 \neq 0)$. Hence $\alpha_1 = 0$ or the characteristic of the field C is two. Then instead of the complicated commutation formula (6)

$$x \cdot a_1 = x^2 - a_1 x + (\gamma_1 - \gamma_2)$$

satisfied by $x = a_1 - a_2$ (cf. Theorem 2), we can construct a simple one by introducing the element t (of the free product P), defined by

$$t = \sqrt{\gamma_2} - a_2 = s_1 - a_2.$$

We now have

$$a_2^2 = (s_1 - t)^2 = s_1^2 - ts_1 - s_1 t + t^2 = \gamma_2,$$

hence

$$ts_1 = t^2 - s_1 t. \tag{36}$$

So we can consider the free product P either as a polynomial ring in x with (6) or as a polynomial ring in t with (36), where the left-hand coefficients are taken from the field K_1. In this case we actually have the free product of two isomorphic quadratic extensions, cf. Cohn [6], p. 551.

By easy calculations we find

$$\left\{ \begin{array}{ll} t(\alpha + \beta a_1) = \beta_1^{-1}\beta t^2 + (\alpha - \beta a_1)t & (\alpha, \beta \in C), \\ t \cdot a = \beta_1^{-1}(aD_1S_1)t + (aS_1)t & (\text{all } a \in K_1). \end{array} \right. \tag{37}$$

Summing up the results we have that the free product P may be considered either as a polynomial ring

$$P = K_1[x; D_1S_1, S_1, (\gamma_1 - \gamma_2)D_1S_1] \tag{38}$$

or as a skew polynomial ring

(39) $$P = K_1[t; \beta_1^{-1} D_1 S_1, S_1, 0],$$

the last type of ring has been studied extensively in [24].

Examples of this first case can easily be given.

E.g. let K_1 be the field of complex numbers over the real number field C, so $a_1 = i$, $\gamma_1 = -1$. Let $\gamma_2 = -d$ $(d > 0)$, then

$$s_1 = \sqrt{\gamma_2} = \sqrt{d}\, i = \beta_1 i \in K_1.$$

Or let K_1 be the field of Laurent series $F\langle\langle s\rangle\rangle$ in the indeterminate s over a ground field F of characteristic 2 (the series contains only a finite number of terms with negative powers of the s), say F is the field of two elements. If γ_2 is not a Laurent series in s^4, then $\sqrt{\gamma_2} = s_1 \notin C$ and s_1 can replace s as basis element of the field K_1 over the subfield $C = F\langle\langle s^2\rangle\rangle$ and the above results may be applied.

2. $\sqrt{\gamma_2}$ does not exist in the field K_1. E.g. K_1 is the complex number field over the rational number field C $(\gamma_1 = -1)$ and $\gamma_2 = 2$ or $\gamma_2 = -2$.

Observe that in both cases R_2 is a quadratic extension field, so the free product P is a PID, cf. (6) and [24], p. 224 or cf. Cohn [6], p. 549, Lemma 2. Also the free product P has a field of right (or left) quotients $Q(P)$, which is a cyclic division algebra, of order 4 over its center, cf. Theorem 5. The actual difficulties arise in the following two cases.

3. $\sqrt{\gamma_2} = \varrho \in C$, $a_2^2 = \gamma_2 = \varrho^2 \neq 0$. The ring R_2 already contains idempotents, e.g.

$$e = (2\varrho)^{-1}(a_2 + \varrho) \text{ and } \bar{e} = (1 - e) = (2\varrho)^{-1}(-a_2 + \varrho).$$

From elementary algebra we know that

$$R_2 = eR_2 \oplus (1-e)R_2 = eC \oplus (1-e)C \cong C \oplus C,$$

i.e. the ring R_2 is the direct sum of two isomorphic copies of the field C. Such a ring has been called a semi-field by Albert [2], p. 81. Of course elements as

$$\gamma_1^{-1} a_1 e a_1$$

are also idempotents in P (not in R_2). Although the ring R_2 does not contain nilpotent elements the free product P of K_1 and R_2 has nilpotent elements, e.g.

$$(a_2 + \varrho) b (a_2 - \varrho), \qquad (b \in P,\, b \notin \text{centre of } P).$$

4. $\sqrt{\gamma_2} = 0$, so $a_2^2 = 0$. The 2-sided ideal $N = a_2 R_2$ of the ring R_2 satisfies

$$N^2 = 0, \;\; R_2/N \cong C,$$

i.e. R_2 is a completely primary ring.

Every element

$$a_2ba_2, \qquad (b \in P, b \notin \text{centre of } P)$$

is nilpotent, as well as every element

$$za_2, \qquad (z \in C[x^2], \text{ the centre of } P).$$

Extensive calculations result in the fact that the free product P does not contain any idempotent (except 1). However the quotient ring $Q(P)$ of P contains infinitely many idempotents, because $Q(P)$ turns out to be a matrix ring over a division ring, cf. FAITH [10], p. 94, the remark under C.

In the last two cases the general structure of the idempotent and nilpotent elements seems to be rather difficult [1]), however in the following section we shall derive some results by which the ring P belongs to a narrow class of rings.

§ 5. THE FREE PRODUCT P OF THE FIELD $K_1 = C(\sqrt{\gamma_1})$ AND THE RING $R_2 = C[\xi]/(\xi^2 - \varrho^2)$.

So let $\gamma_2 = \varrho^2$ where ϱ is allowed to be equal to zero. From the Theorems 1 and 2 we immediately see that P is a left (and by symmetry also a right) Noetherian prime ring, so certainly the ring P is nil semi-simple. By the same two theorems we also conclude that the (left) quotient ring $Q(P)$ of P is a left (and right) Artinian simple ring, hence a complete matrix ring over a division ring, i.e. a (left and right) principal ideal ring, cf. JACOBSON [14], p. 75. Summing up the results we have

Theorem 6. The free product $P = C(\sqrt{\gamma_1}) \star C[\xi]/(\xi^2 - \varrho^2)$ is a Noetherian prime ring and its quotient ring $Q(P)$ is a complete matrix ring over a division ring, so a principal ideal ring.

The properties of $Q(P)$ could also be derived from Theorem 5. There we obtained that the quotient ring $Q(P)$ of P may be considered as a cyclic algebra

$$Q(P) = (E, S, \gamma_2)$$

over the cyclic field E and also as an algebra of order 4 over its center $C(x^2)$. If $\gamma_2 = \varrho^2$ then

$$Q(P) = (E, S, \varrho^2)$$

is a total matrix algebra, cf. ALBERT [1], Theorem 6, ALBERT [2], p. 75 or HASSE [11], p. 199.

When we apply ALBERT [2, V, Theorem 11] we can even find more than Theorem 6. Namely let C be the field of rational numbers and write $\varrho^2 = \varrho_1\varrho_2$, where ϱ_1 and ϱ_2 are no perfect squares. Then we can derive

$$Q(P) = (E, S, \varrho^2) = (E, S, \varrho_1 \cdot \varrho_2) = (E, S, \varrho_1) \otimes (E, S, \varrho_2).$$

[1]) The author wishes to thank Professor A. W. Goldie for some stimulating discussions on these subjects.

Thus the quotient ring $Q(P)$ of the free product is the tensor (direct) product of two cyclic division algebras of order 4 over its center, cf. Theorem 5. Summing up the results we have the following completion of Theorem 6.

Theorem 7. If γ_2 is a square and C is the rational number field, then the quotient ring $Q(P)$ of P is the tensor (direct) product of two cyclic division algebras of order 4 over its center $C(x^2)$.

From Theorem 6 we know that $Q(P)$ is a complete matrix ring over a division ring. Which division ring? Theorem 7 gives us the feeling that this division ring will be $C(x^2)$, the (commutative) field of fractions of the polynomial ring $C[x^2]$. However this becomes more clear in the following section.

§ 6. Matrix representations

It is not difficult to get a matrix representation for the free product P of the field K_1 and the ring $R_2 = C[\xi]/(\xi^2 - \varrho^2)$. We copy the method from Jacobson [13], p. 205. Let X denote the matrix

$$\begin{pmatrix} 1 \\ x \end{pmatrix}$$

and let

$$g = a + bx \qquad (a, b \in A = K_1[x^2])$$

be an arbitrary element of the free product P, cf. Theorem 2. Then the relations

$$1(a+bx) = a + bx$$
$$x(a+bx) = \bar{a} + \bar{b}x \qquad (\bar{a}, \bar{b} \in A)$$

may be written as

$$\begin{pmatrix} 1 \\ x \end{pmatrix} (a+bx) = \begin{pmatrix} a & b \\ \bar{a} & \bar{b} \end{pmatrix} \begin{pmatrix} 1 \\ x \end{pmatrix},$$

in short $Xg = GX$.

The correspondence $g \to G$ is readily verified to be an isomorphism. E.g. we have

$$\text{(I)} \quad x = a_1 - a_2 \to \begin{pmatrix} 0 & 1 \\ x^2 & 0 \end{pmatrix}, \; a_1 \to \begin{pmatrix} a_1 & 0 \\ x^2 + \gamma_1 - \gamma_2, & -a_1 \end{pmatrix}, \; a_2 \to \begin{pmatrix} a_1 & -1 \\ \gamma_1 - \gamma_2, & -a_1 \end{pmatrix}$$

and with $\gamma_2 = \varrho^2$ and a few manipulations we "easily" come on the representation

$$\text{(II)} \quad x = a_1 - a_2 \to \begin{pmatrix} 0 & 1 \\ x^2 & 0 \end{pmatrix}, \; a_1 \to \begin{pmatrix} \varrho & 1 \\ \gamma_1 - \varrho^2, & -\varrho \end{pmatrix}, \; a_2 \to \begin{pmatrix} \varrho & 0 \\ \gamma_1 - \varrho^2 - x^2, & -\varrho \end{pmatrix}.$$

The last representation is a representation of the free product P in the matrix algebra of order 4 over the ring $C[x^2]$. We observe that P

is not represented by the complete matrix ring over $C[x^2]$, for then P would be a principal ideal ring, which is not the case (cf. JACOBSON [14], Theorem 40).

However, the quotient ring $Q(P)$ of P is the total matrix algebra over the field $C(x^2)$, which proves the statements at the end of the previous section. Summing up the results just obtained we have

Theorem 8. If $\gamma_2=\varrho^2$ ($\varrho \in C$), then the quotient ring $Q(P)$ of the free product P may be considered as the complete ring of 2×2 matrices over the field $C(x^2)$. The free product P itself may be considered as a ring (not the complete ring) of 2×2 matrices over the ring $C[x^2]$, the center of P.

Final remarks. Replacing ϱ by $-\varrho$ the representation (II) appears to be equivalent to the representation

$$\text{(III)}\quad x=a_1-a_2 \to \begin{pmatrix} -\varrho & x^2-\varrho^2 \\ 1 & \varrho \end{pmatrix},\ a_1 \to \begin{pmatrix} 0 & \gamma_1 \\ 1 & 0 \end{pmatrix},\ a_2 \to \begin{pmatrix} \varrho & \gamma_1+\varrho^2-x^2 \\ 0 & -\varrho \end{pmatrix}.$$

This representation of the free product P may also be obtained from Theorem 4, however we shall not derive this representation in detail here.

If $D=C(x^2)$ then we know that the free product P has a quotient ring $Q(P)=D_2$, the complete 2×2 matrix ring over the field D. Further let F be the subring of D defined by

$$F=\{x^4-2(\gamma_1+\gamma_2)x^2+(\gamma_1-\gamma_2)^2\}C[x^2]=(y^2-4\gamma_1)C[x^2],$$

i.e. F is a principal 2-sided ideal in the ring $C[x^2]\subset D$. Now we can prove that the Noetherian prime ring P contains the subring

$$F_2=\begin{pmatrix} F & F \\ F & F \end{pmatrix},$$

which is a nice illustration of the Faith-Utumi Theorem, cf. [10], p. 91 or [20], p. 610.

As far as the author can observe now the Noetherian prime ring P is not a maximal order in its quotient ring $Q(P)$ and is also not a Dedekind ring in the sense of ROBSON, cf. [21]. But the structure of the ring is too beautiful to have no "regular" arithmetic of ideals. We hope to deal with these problems in a further communication.

Department of Mathematics
Delft, University of Technology
The Netherlands

REFERENCES

1. ALBERT, A. A., On the construction of cyclic algebras with a given exponent. Am. J. of Math. 54, 1–13 (1932).
2. ————, Structure of algebras. Amer. Math. Soc., Providence, R.I. (1939).
3. AMITSUR, S. A., Non-commutative cyclic fields. Duke Math. J. 21, 87–105 (1954).

4. Cohn, P. M., On the free product of associative rings. Math. Z. **71**, 380–398 (1959).
5. ————, On the free product of associative rings. The case of (skew) fields. Math. Z. **73**, 433–456 (1960).
6. ————, Quadratic extensions of skew fields. Proc. London Math. Soc. (3) **11**, 531–556 (1961).
7. ————, Rings with a weak algorithm. Trans. Am. Math. Soc. **109**, 332–356 (1963).
8. ————, Free ideal rings. Journal of Algebra (1) **1**, 47–69 (1964).
9. Divinsky, N. J., Rings and radicals. George Allen & Unwin Ltd, London (1965).
10. Faith, C., Lectures on injective modules and quotient rings. Springer-Verlag, Berlin (1967).
11. Hasse, H., Theory of cyclic algebras over an algebraic number field. Trans. Am. Math. Soc. **34**, 171–214 (1932).
12. Herstein, I. N., Noncommutative rings. The Carus Math. Monographs (Number 15), 1968.
13. Jacobson, N., Non-commutative polynomials and cyclic algebras. Ann. of Math. **35**, 197–208 (1934).
14. ————, Theory of rings. Amer. Math. Soc., Providence, R.I. (1943).
15. ————, Structure of rings. Amer. Math. Soc., Providence, R.I., 1956, 1964 (revised edition).
16. Latimer, C. G., On the finiteness of the class number in a semi-simple algebra. Bull. Am. Math. Soc. **40**, 433–435 (1934).
17. ————, On ideals in generalized quaternion algebras and Hermitian forms. Trans. Am. Math. Soc. **38**, 436–446 (1935).
18. ————, On the class number of a quaternion algebra with a negative fundamental number. Trans. Am. Math. Soc. **40**, 318–323 (1936).
19. Robson, J. C., Pri-rings and ipri-rings. Quarterly J. of Math. (70) **18**, 125–145 (1967).
20. ————, Artinian quotient rings. Proc. London Math. Soc. (3) **17**, 600–616 (1967).
21. ————, Non-commutative Dedekind rings. Journal of Algebra **9**, 249–265 (1968).
22. Shover, G., Class number in a linear associative algebra. Bull. Am. Math. Soc. **39**, 610–614 (1933).
23. Smits, T. H. M., Nilpotent S-derivations. Proc. Kon. Ned. Akad. Wetensch. **A 70** (=Indag. Math. **30**), 72–86 (1968).
24. ————, Skew polynomial rings. Proc. Kon. Ned. Akad. Wetensch. **A 71** (=Indag. Math. **30**), 209–224 (1968).
25. Faith, C. and Y. Utumi, On noetherian prime rings. Trans. Am. Math. Soc. **114**, 53–60 (1965).